(51) International Patent Classification⁷: G06F 9/445,
H04L 9/00

(21) International Application Number:
PCT/AU2004/001267

(22) International Filing Date:
17 September 2004 (17.09.2004)

(25) Filing Language: English

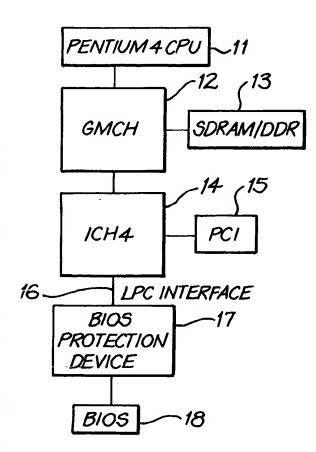(26) Publication Language: English

(30) Priority Data:
2003905097   18 September 2003 (18.09.2003)   AU

(71) Applicant (for all designated States except US): ARIS-
TOCRAT TECHNOLOGIES AUSTRALIA PTY LTD
[AU/AU]; 71 Longueville Road, Lane Cove, NSW 2066
(AU).

(72) Inventor; and
(75) Inventor/Applicant (for US only): MUIR, Robert, Lin-
ley [AU/AU]; C/-85-113 Dunning Ave, Rosebery, NSW
2018 (AU).

(74) Agent: F B RICE & CO; 605 Darling Street, Balmain,
NSW 2041 (AU).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,
MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG,
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,
ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,

(54) Title: BIOS PROTECTION DEVICE

(57) Abstract: A processing system including a bios protection
device and method of protecting a bios is provided. The system
comprises a central processor (11), and a BIOS memory device
(18) to which the BIOS protection device (17) is interconnected
by address and data paths (16). At start-up, the BIOS protec-
tion device (17) takes control of the memory address and data
paths (16) and prevents execution of a boot program stored in the
BIOS memory device (18) until the BIOS protection device (17)
has verified that the boot program stored in the BIOS memory
device (18) is authentic. The BIOS protection device (17) is con-
nected to the processing system between a central processor (11)
and the BIOS memory device (18), and includes address and
data path interface connection means (24, 25), and an authenti-
cation processor (21). When power is applied to the BIOS pro-
tection device (17), the BIOS protection device (17) takes con-
trol of address and data path(s) (16) to which it is connected and
the authentication processor (21) interrogates the BIOS mem-
ory device (18) connected to the address and data path(s) (16)
to determine if the boot program contained in the BIOS mem-
ory device (18) is authentic. Only if the boot program is de-
termined to be authentic does the BIOS protection device (17)
release control of the address and data path(s) (16) to permit the
central processor (11) to execute the boot program.

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.